RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: IMT-R01

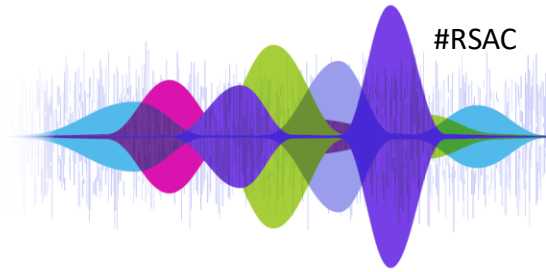
Dr. Darkness or: How We Learned to Stop Worrying and Love Downtimes

Aaron Weismann

Chief Information Security Officer
Main Line Health
https://www.linkedin.com/in/aaron-weismann-4a468247/

Tony Fiore

Program Manager
Main Line Health
https://www.linkedin.com/in/anthonytfiore/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- Why we embraced existential organizational downtimes
- Our iterative approach to disaster preparedness
- The many benefits from disaster preparedness planning

RSAC 2025 Conference

Why we embraced existential organizational downtimes

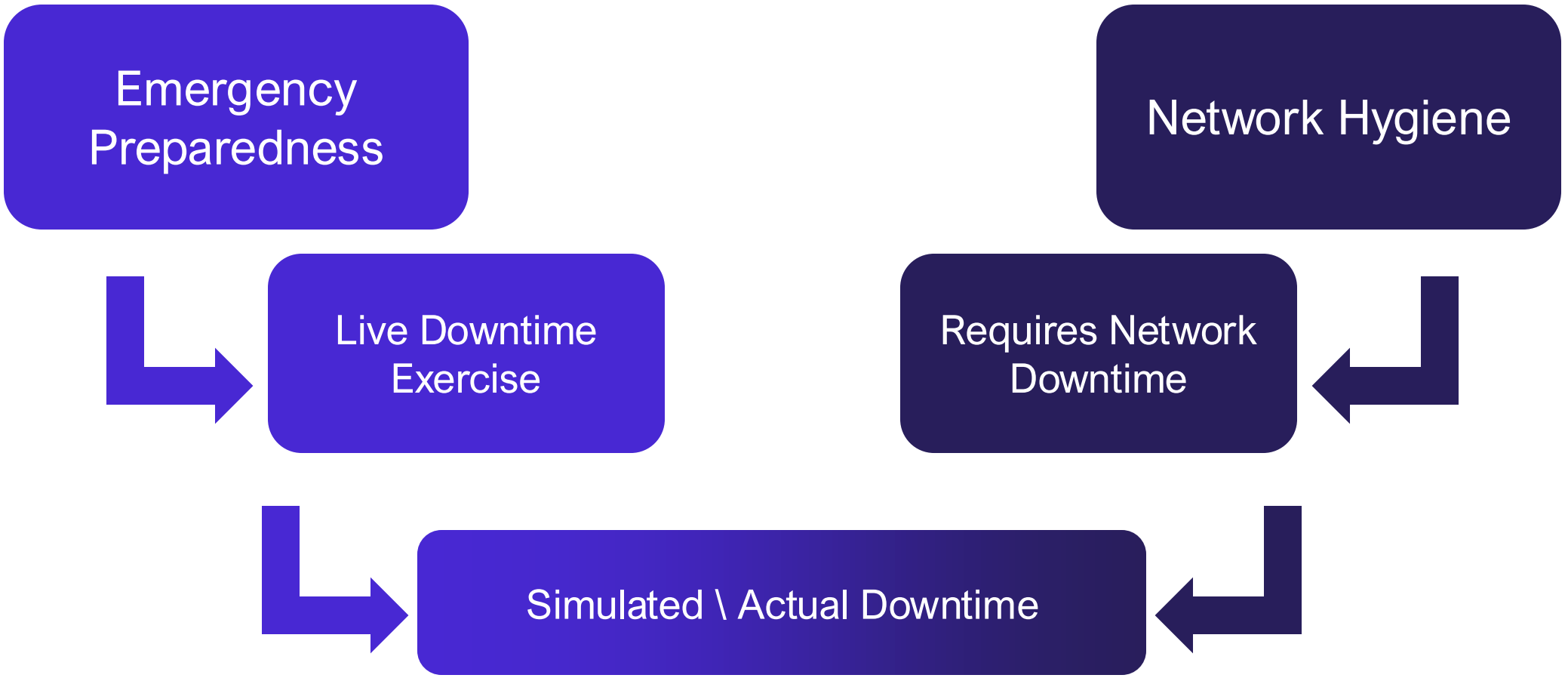
Iteration 1

Many Voices.
One Community.

Cyberattacks prey on impacts to modern patient care because diminished patient outcomes are a strong motivator to pay a ransom.

- Ransomware attacks doubled in 2023 compared to 2022 – cybercriminals are making billions of dollars a year on the healthcare industry.
- The average institutional downtime is greater than a month and this directly translates into diminished patient outcomes, reputational risks, and financial risks.
- Multiple extortion is popular: 1) Ransom an institution to unencrypt systems and resume business, 2) ransom an institution not to leak data, 3) ransom an institution not to report the breach caused by the cybercriminal.
- It's a matter of when and not if. A sufficiently sophisticated cybercriminal will compromise any system.

Our downtime preparedness program started at the intersection of two different projects



We embraced the need for Digital Darkness using the principles of Chaos Engineering to drive progress

- **Chaos engineering** is the practice of intentionally injecting faults into a system to test its resilience.
- **Digital darkness** would show us where downtime transition execution would have gaps.
- We also anticipated that forced, controlled digital darkness would highlight “unknown unknowns” vis a vis infrastructure gaps.

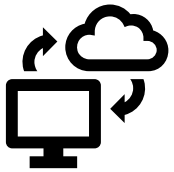
Challenges and Lessons Learned

Coordination of bedside care teams

Practice using downtime forms – tabletop at the unit

Work with physician leadership to educate

Emergency continuity infrastructure required modification to function effectively



Literally any technology and Electronic Medical Record ("EMR") connectivity is preferable to no technology

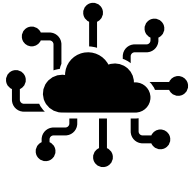
RSAC 2025 Conference

Our iterative approach to disaster preparedness

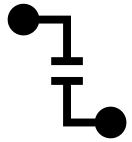
Iteration 2

Many Voices.
One Community.

Pivot Principles

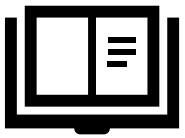


Technology is key



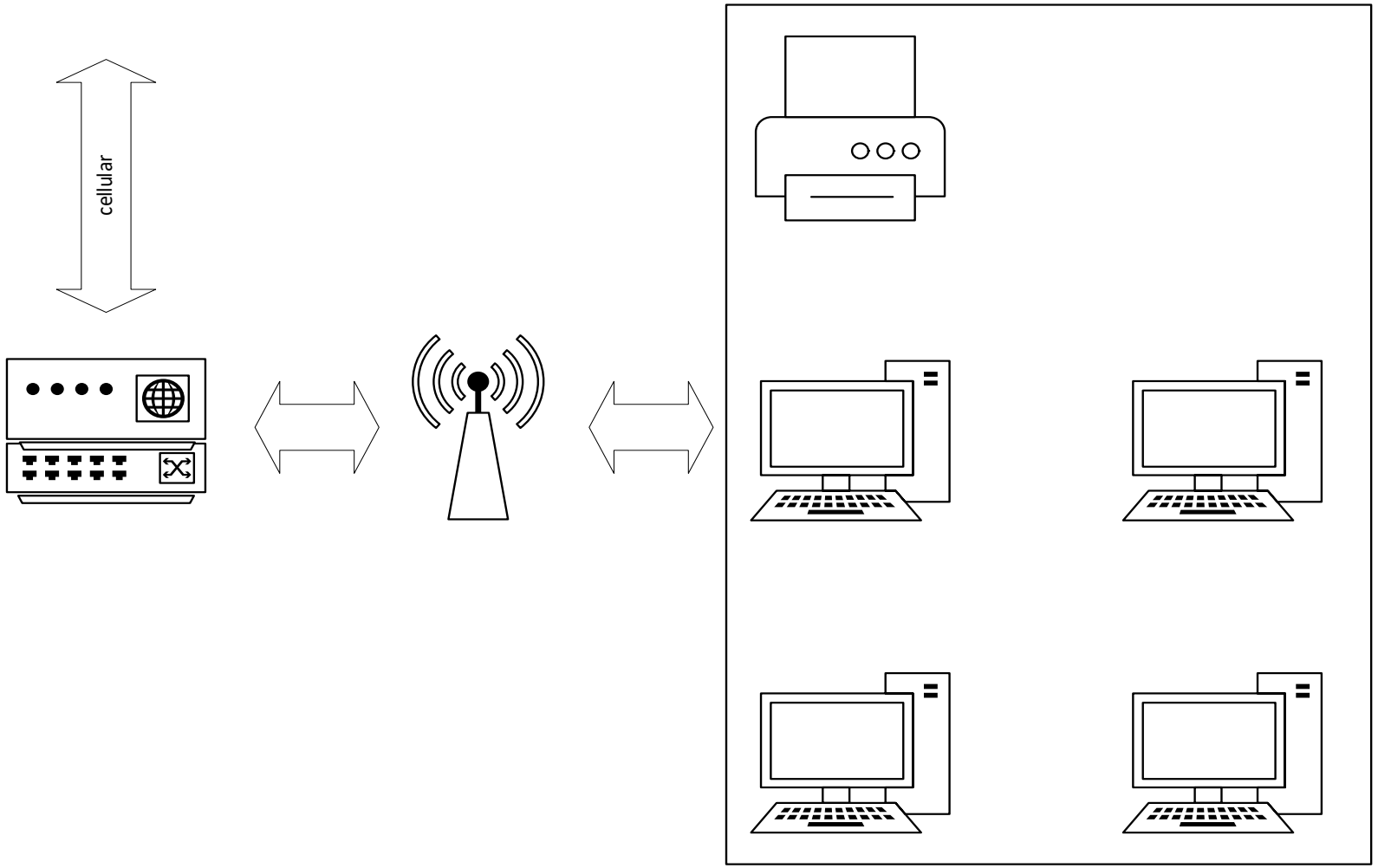
Completely air-gapped recovery infrastructure

Self-support for non-technological staff



Paper processes are our final backstop

Per-unit disaster technology architecture



Air-gapped technology with a distinct architecture from production means no cross-infection from ransomware

cradlepoint

PART OF ERICSSON

Distinct Cellular Network

chromeOS

Distinct OS

Absolute baseline “must-haves” for safe continuity of patient care

Epic

Human-centric design principles dictated the platform for technology continuity

+

=

Workstations on wheels are a familiar commodity to clinical staff, and we provide a second life to equipment not fit for direct patient care

What about external third-party service downtime?

Paper, paper, paper! We are doubling down on our paper process training as a backstop. Every clinical operator will receive digital interactive paper charting training.

We discuss and document system outage plans and prepare manual processes.

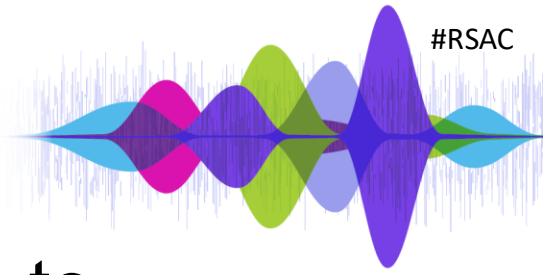
We're upfront and collaborative in conversations with vendors; preparing now means less finger-pointing later.

It's not going to be perfect, and the unknown unknowns will hurt. Internal collaboration is key.

RSAC™ | 2025 Conference

The many benefits from disaster preparedness planning

Robust clinical operations conversations



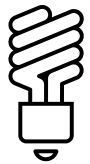
- No two hospitals in our system have the same approach to operational resilience
  - Our goal is to work with clinical operations to standardize perception and approach
- Paper is never disappearing
  - We can make training engaging and interactive while deploying to the entire enterprise
- Resilience can be built into our operational identity
  - As we expand as a system we can do so resiliently

Process improvement

This project was entirely about failing fast and pivoting agilely

There’s no one-size-fits-all solution, but we can generalize

Business operations loves collaborating on technology innovation



Technology enables better operations

Driving partnerships

Information Security

Enterprise Applications

Biomedical Operations

Disaster Preparedness Planning

Clinical Operations

Finance

Epic

“Apply” Slide

- Next week you should:
  - Identify the business services without which your organization genuinely cannot continue operations
  - Begin conversations with business operations counterparts to instill an appreciation of what a complete downtime means
- In the first three months following this presentation you should:
  - Architect a plan for preserving those business services in the event of catastrophic, total downtime
  - Meet with critical service providers to plan for continuity of operations
- Within six months you should:
  - Begin pressure testing your disaster approach